Kapitola: Gödelova veta o neúplnosti

1.1 Jazyk logiky

Cieľ: Voľne povedané, chceme mať formálny systém, v ktorom budeme vedieť dokazovať matematické tvrdenia zodpovedajúce práve všetkým pravdivým tvrdeniam nášho sveta. V ideálnom prípade by sme teda chceli zostrojiť mechanický proces, ktorého vstupom bude tvrdenie a výstupom buď dôkaz tohto tvrdenia, alebo dôkaz jeho negácie. Toto je v podstate cieľ, ktorý ako prvý sformuloval už pred niekoľkými storočiami Leibniz, a neskôr v roku 1920 v omnoho exaktnejšej podobe Hilbert.

Začať musíme tým, že si zvolíme nejakú konečnú abecedu, pomocou ktorej budeme tieto tvrdenia zapisovať. (Niektorí autori si volia abecedu spočítateľne nekonečnú, lebo je to pohodlnejšie a aj tak ju vieme zakódovať pomocou konečnej.) Symboly tejto abecedy budeme pre názornosť v tomto texte uvádzať vizuálne odlišným písmom: x, ∀, 0, atď.

My sa na tieto reťazce budeme pozerať a niektorým z nich priradíme *význam* – budú zodpovedať tvrdeniam v našom svete. Bude pohodlné nepriradzovať význam všetkým reťazcom, niektoré pre nás budú jednoducho nezmyselné postupnosti znakov.

Príklad 1: x∀0→ môže pre nás byť nezmyselná postupnosť znakov, zatiaľ čo ∃z(47=z+z) môže predstavovať tvrdenie „47 je párne číslo“.

Príklad 2: Rovnako dobre sa však môžeme dohodnúť, že reťazec ∀0 predstavuje reláciu „väčší alebo rovný“ a symbol → číslo 7. Potom by reťazec x∀0→ predstavoval tvrdenie „x je väčšie alebo rovné ako 7“, zatiaľ čo ∃z(47=z+z) môže pre nás byť nezmyselná postupnosť znakov.

Poučenie: Samotné reťazce nemajú žiaden svoj inherentný zmysel, ten im dávame až my, ktorí sa na ne pozeráme „zvonka“.

Keď budeme navrhovať konkrétny formálny systém, množina všetkých jeho reťazcov, ktoré budeme považovať za syntakticky korektné, musí byť dostatočne jednoduchá. Zjavná minimálna požiadavka je, že chceme vedieť o ľubovoľnom reťazci mechanicky rozhodnúť, či je alebo nie je syntakticky korektný. Inými slovami, zaujímať nás budú len také formálne systémy, pre ktoré je množina syntakticky korektných reťazcov rekurzívna.

1.2 Predikátová logika prvého rádu

Predikátová logika je formálny systém, v ktorom niektoré symboly abecedy interpretujeme ako *premenné*, niektoré ako *logické spojky*, niektoré ako *kvantifikátory*, niektoré ako *zátvorky* a niektoré ako *predikáty*. (Nič nám nezakazuje mať ešte ďalšie symboly, ktoré budeme interpretovať ešte ináč, napr. ako konštanty alebo funkcie.)

Upresnenie, že hovoríme o logike prvého rádu, má nasledujúci význam: za korektné reťazce budeme považovať len tie, kde sa každý kvantifikátor viaže na nejakú premennú. V logike prvého rádu teda vieme formalizovať napr. tvrdenie „pre všetky x existuje y také, že...“, ale nevieme formalizovať napr. tvrdenie „existuje predikát p, pre ktorý platí...“.

1.3 Formalizácia aritmetiky po prvé

V tejto časti budeme uvažovať jednoduchú formalizáciu aritmetiky v predikátovej logike prvého rádu. Zatiaľ nebudeme zachádzať do detailov a popíšeme len tie časti tejto formalizácie, ktoré potrebujeme.

Jazyk našej aritmetiky postavíme nad abecedou obsahujúcou okrem iného symboly 01+*=¬∧∨→∀∃(). Všetkým týmto symbolom priradíme ich bežné významy. Okrem nich budeme ešte mať symboly xyz označujúce premenné. (Keby sme ich niekedy potrebovali viac, môžeme sa napr. dohodnúť, že každý neprázdny reťazec týchto symbolov predstavuje premennú.)

Množinu syntakticky korektných reťazcov nášho jazyka aritmetiky budú tvoriť formálne zápisy korektných tvrdení v aritmetike prirodzených čísel.

Do tejto množiny napríklad patria reťazce $\forall$x(∀y(x+y=y+x)), $\forall$x(∀y((x*y=0)→((x=0)∧(y=0)))) aj $\exists$y(x=y+y). Prvý z nich zodpovedá pri našej interpretácii symbolov pravdivému tvrdeniu „sčítanie je komutatívne“, druhý nepravdivému tvrdeniu „ak súčin x a y je 0, tak sú oba rovné 0“ a tretí tvrdeniu „x je párne číslo“, ktoré samo o sebe pravdivostnú hodnotu nemá.

Pri práci s takýmto systémom sa nám často oplatí zjednodušiť si život tým, že zavedieme nové symboly, ktoré budú predstavovať konkrétne reťazce. Tieto nové symboly teda treba chápať rovnako ako napr. makrá v bežných programovacích jazykoch. V našom jazyku sa môžeme napríklad dohodnúť na týchto makrách:

X<Y je skrátený zápis pre $\exists$z(¬(z=0)∧((X)+z=(Y)))

2 je skrátený zápis pre (1+1), 3 je skrátený zápis pre ((1+1)+1), atď.

Všimnite si, že 3 **nie je** skrátený zápis pre (1+(1+1)). Čo sa reťazcov týka, ((1+1)+1) a (1+(1+1)) sú dva rôzne reťazce.

Označme teraz $\mathcal{T}$ jazyk tých reťazcov, ktoré sú syntakticky korektné a keď ich interpretujeme v našom jazyku ako tvrdenia o prirodzených číslach, tak zodpovedajú pravdivým tvrdeniam. Analogicky označme $\mathcal{F}$ jazyk tých reťazcov, ktoré zodpovedajú nepravdivým tvrdeniam.

Príklad: reťazec $\forall$x(∀y(x+y=y+x)) patrí do $\mathcal{T}$, reťazec $\forall$x(∀y((x*y=0)→((x=0)∧(y=0)))) do $\mathcal{F}$ a reťazec $\exists$y(x=y+y) nepatrí ani do jednej z týchto množín.

Množina $\mathcal{T}$ je to, čo nás matematikov zaujíma – do formálneho jazyka zakódovaná množina všetkých pravdivých tvrdení.

1.4 Sila aritmetiky so sčítaním a násobením

Zdôvodníme si teraz, že ku každému rekurzívnemu predikátu existuje v našom formálnom systéme reťazec, ktorý mu zodpovedá. Upozorňujeme, že nejde o formálny dôkaz v žiadnom formálnom systéme, ale o zdôvodnenie v našej realite (metamatematike).

Presnejšie, ukážeme, že k ľubovoľnému rekurzívnemu predikátu $P(x_1, \ldots, x_n)$ existuje reťazec R_P obsahujúci voľné premenné x, ..., $\mathtt{x}^n$ taký, že pre ľubovoľné $a_1, \ldots, a_n \in \mathbb{N}$ platí: $P(a_1, \ldots, a_n)$ vráti 1 práve vtedy, keď do $\mathcal{T}$ patrí reťazec, ktorý dostaneme z R_P tak, že pre každé k za každý výskyt $\mathtt{x}^k$ dosadíme reťazec zodpovedajúci číslu a_k. (Poznámka: značenie $\mathtt{x}^n$ tu predstavuje reťazec tvorený n písmenami x.)

Detaily zdôvodnenia prenecháme na čitateľa, načrtneme len myšlienku. Zdôvodníme všeobecnejšie tvrdenie: ku každej rekurzívnej funkcii $f(x_1, \ldots, x_n)$ existuje reťazec R_f obsahujúci voľné premenné y, x, ..., $\mathtt{x}^n$ ktorý vo vyššie popísanom zmysle zodpovedá predikátu $y = f(x_1, \ldots, x_n)$.

Zdôvodnenie prebieha štrukturálnou indukciou – inými slovami, postupne čítame „recept“ funkcie f a podľa neho zostrojujeme príslušný reťazec.

Pre základné funkcie zostrojíme reťazce ľahko: Funkcii $z()$ zodpovedá reťazec y=0. Funkcii $s(x)$ zodpovedá reťazec y=x+1. Projekcii P_k^n zodpovedá reťazec $\mathtt{y}=\mathtt{x}^k$.

Nech funkcia $f(x_1, \ldots, x_n)$ vzniká kompozíciou funkcií $g(x_1, x_2)$, $h_1(x_1, \ldots, x_n)$ a $h_2(x_1, \ldots, x_n)$. Nech ďalej g, h_1 a h_2 majú zodpovedajúce reťazce R_g, R_{h1} a R_{h2}. BUNV predpokladajme, že tieto reťazce neobsahujú výskyty premenných yy a yyy (inak dotyčné premenné premenujeme). Potom funkcii f zodpovedá nasledujúci reťazec:

$$\forall\mathtt{yy}\,(\forall\mathtt{yyy}\,(\ R_{h1}(\mathtt{yy}, \mathtt{x}, \ldots, \mathtt{x}^n)\ \wedge\ R_{h2}(\mathtt{yyy}, \mathtt{x}, \ldots, \mathtt{x}^n)\ \rightarrow\ R_g(\mathtt{y}, \mathtt{yy}, \mathtt{yyy})\ ))$$

Reťazec $R_{h1}(\mathtt{yy}, \mathtt{x}, \ldots, \mathtt{x}^n)$ vznikne tak, že za každý výskyt voľnej premennej y v R_{h1} dosadíme yy. Analogicky dosadíme yyy do R_{h2}. Reťazec $R_g(\mathtt{y}, \mathtt{yy}, \mathtt{yyy})$ vznikne z R_g tak, že za všetky výskyty voľnej premennej x dosadíme yy a za všetky výskyty xx dosadíme yyy.

Slovne, zostrojený výraz zodpovedá tvrdeniu: „Ak yy a yyy sú hodnoty, ktoré vrátia h_1 a h_2 pre zadané x, ..., $\mathtt{x}^n$, tak nutne g pre vstup yy, yyy musí vrátiť hodnotu y.“ Ľahko nahliadneme, že toto tvrdenie je naozaj ekvivalentné s tvrdením „f pre vstup x, ..., $\mathtt{x}^n$ vráti výstup y.“

Konštrukcia pre kompozíciu v prípade inej arity g vyzerá analogicky, a konštrukciu pre prípad, že f vzniká regulárnou minimalizáciou, prenechávame na čitateľa.

1.5 Aká zložitá je pravda?

V tejto časti ukážeme, že množina $\mathcal{T}$ pravdivých tvrdení v našej aritmetike prirodzených čísel nie je ani len rekurzívne vyčísliteľná.

Zoberme našu starú známu množinu $HALT$. Zjavne existuje rekurzívny predikát $H(x, y)$ taký, že $x \in HALT$ práve vtedy, keď $\exists y H(x, y)$. (Napr. môžeme zvoliť $H(x, y) =$„vieme vypočítať hodnotu $f_x(x)$, ak smieme spraviť nanajvýš y krokov výpočtu?“) Keďže H je rekurzívny predikát, existuje reťazec R_H, ktorý mu zodpovedá.

Uvažujme teraz funkciu p, ktorá robí nasledujúce: ak na vstupe dostane číslo n, tak na výstupe vypíše reťazec $\neg\exists\mathrm{y}\,(\;R_H(n,\mathrm{y})\;)$.

Funkcia p je zjavne rekurzívna – len zoberie reťazec R_H, všetky výskyty premennej x nahradí reťazcom zodpovedajúcim číslu n a následne okolo toho pridá niekoľko ďalších znakov.

A tiež zjavne platí $n \in \overline{HALT} \iff p(n) \in \mathcal{T}$ – totiž p pre n vyrobí tvrdenie „neexistuje y také, že výpočet $f_n(n)$ zastane po nanajvýš y krokoch“, čo je ekvivalentné s tvrdením „výpočet $f_n(n)$ nezastane“, a teda v $\mathcal{T}$ je tento reťazec naozaj práve vtedy, keď $n \in \overline{HALT}$.

A tým sme naše zdôvodnenie ukončili – zostrojená p je totiž many-to-one redukciou $\overline{HALT}$ na $\mathcal{T}$, a teda $\mathcal{T}$ nie je ani len rekurzívne vyčísliteľná.

Toto je smutné zistenie. Hovorí nám, že neexistuje program, ktorý by generoval pravdivé aritmetické tvrdenia a časom vygeneroval každé z nich.

1.6 Jednoduchý pohľad na formálne dokazovanie

Zatiaľ sme sa zaoberali len otázkou, čo je pravdivé. Samotná pravdivosť tvrdenia nám matematikom ale často nestačí, my chceme vidieť pod pokrievku. Rozumieť nie len tomu, či niečo funguje, ale tiež tomu, ako a prečo. A práve toto nás privádza k pojmu *dôkazu*.

Ponechajme zatiaľ bokom „implementačné detaily“, teda to, ako vlastne dokazujeme a čo to ten dôkaz je. Zatiaľ nám postačí sústrediť sa na esenciu dôkazu. Čo je to dôkaz tvrdenia T? To je nejaký reťazec D_T, ktorý vieme mechanicky spracovať, skontrolovať, a ak všetko sedí, tak nás ten reťazec presvedčí o tom, že T platí.

Inými slovami, požadujeme, aby existoval rekurzívny predikát $D(x, y)$, ktorý nám povie, či je reťazec y dôkazom reťazca x.

No a už tu sa dostávame do zjavných problémov. Pripomeňme si, že v predchádzajúcej časti sme si dokázali, že množina pravdivých tvrdení v našej aritmetike prirodzených čísel nie je ani len rekurzívne vyčísliteľná. Množina dokázateľných tvrdení naopak rekurzívne vyčísliteľná vždy bude. (Pre konkrétne tvrdenie x vieme skúšať postupne všetky možné y a akceptujeme, ak nájdeme také y, pre ktoré platí $D(x, y)$.)

Z toho vyplýva druhé smutné zistenie: Nech akokoľvek rozumne definujeme, čo je to dôkaz, vždy budú existovať tvrdenia, ktoré budú síce pravdivé, ale nebudeme ich vedieť dokázať.

1.7 Axiómy a teórie

Jedným z cieľov matematiky môže byť zisťovanie právd o našom, reálnom svete. Ani zďaleka napríklad ešte nevieme všetko o prirodzených číslach. (Existuje nepárne dokonalé číslo? Platí Goldbachova domnienka? A čo Riemannova hypotéza?)

Navyše dôkazy zložitých tvrdení (napr. veta o štyroch farbách či veľká Fermatova veta) sú často natoľko komplikované, že nie je zjavné, či niekde neskrývajú chyby.

Preto má zmysel budovať matematiku formálne, axiomaticky: Začneme tým, že sa dohodneme na čo najmenšom počte základných tvrdení, o ktorých sa zhodneme, že v našom svete platia. A následne sa dohodneme na sade odvádzacích pravidiel (napr. modus ponens) o ktorých veríme, že z pravdivých tvrdení vždy vyrobia pravdivé.

V jazyku logiky tento prístup vyzerá nasledovne: Zvolíme si jazyk axióm A. (Tento jazyk by, ak už nič iné, mal byť rekurzívny – inými slovami, chceme vedieť mechanicky rozhodnúť, či daný reťazec zodpovedá v našom svete jednej z dohodnutých axióm alebo nie.) Následne sa dohodnem na sade mechanických prepisovacích pravidiel. Môžeme sa na to dívať napríklad tak, že každé prepisovacie pravidlo je program, ktorý má na vstupe niekoľko (možno aj nula) reťazcov a na výstupe práve jeden nový reťazec.

Napríklad modus ponens by bol program, ktorý ak dostane na vstupe reťazce tvarov `A→B` a `A`, tak vyrobí reťazec `B` – pričom `A` a `B` môžu byť ľubovoľné syntakticky korektné reťazce.

Príkladom prepisovacieho pravidla, ktoré môže mať nula vstupov, je veta o dedukcii (http://en.wikipedia.org/wiki/Deduction_theorem).

Postupným používaním dohodnutých odvádzacích pravidiel vieme následne z axióm vyrábať nové a nové reťazce. Konkrétny spôsob výroby daného reťazca x vieme samozrejme zakódovať ako reťazec y, ktorý potom voláme dôkazom reťazca x.

Keď sa teraz pozeráme čisto syntakticky na nejaký formálny systém, ktorý takto funguje, môžeme hovoriť o jeho *konzistentnosti* a *úplnosti*. Toto sú teraz syntaktické pojmy, bez akéhokoľvek odvolávania sa na modely a pravdivosť. Nech A je množina axióm a $D(x, y)$ rekurzívny predikát „je y dôkazom x z axióm A?“. Potom hovoríme, že dvojica (A, D) je konzistentná, ak neexistuje reťazec taký, že sa dá dokázať aj on, aj jeho negácia. A hovoríme, že dvojica (A, D) je úplná, ak neexistuje reťazec taký, že sa nedá dokázať ani on, ani jeho negácia.

Z vyššie uvedených výsledkov už vieme, že žiaden konzistentný formálny systém, ktorý umožňuje formalizáciu aritmetiky, nemôže byť úplný. Presnejšie nám o tom hovoria Gödelove vety o neúplnosti: Prvá z nich ukazuje, že v takomto formálnom systéme vieme zostrojiť konkrétny reťazec taký, že ani on, ani jeho negácia nie sú dokázateľné. Druhá Gödelova veta následne hovorí, že ďalším (zložitejším) reťazcom s touto vlastnosťou je reťazec, ktorý je formalizáciou tvrdenia „tento formálny systém je konzistentný“.

Čo nám toto hovorí o pravde? Ak veríme našim axiómam a odvádzacím pravidlám, tak ku každému konzistentnému formálnemu systému, ktorý je dostatočne silný na to, aby sa v ňom dala sformulovať aritmetika prirodzených čísel, existuje v našom svete pravdivé tvrdenie, ktorého formalizáciou je reťazec, ktorý v danom systéme nevieme dokázať ani vyvrátiť. A navyše je takýchto tvrdení veľa, a jedným z nich je aj konzistencia daného formálneho systému. V rámci konzistentného formálneho systému obsahujúceho aritmetiku prirodzených čísel teda nikdy nebudeme schopní dokázať jeho konzistenciu.

1.8 Curryho paradox

Potrebu formálneho prístupu si pekne môžeme ukázať na Curryho paradoxe. Uvažujme nasledovný výrok: „Ak je tento výrok pravdivý, tak skúšku z vypočítateľnosti nik nespraví.“ Toto je implikácia, teda výrok „ak A, tak B“. Dokážeme ho priamo: predpokladáme, že platí A, a odvodíme B.

Lenže čo je to A? A je „tento výrok“, a teda A je „Ak je tento výrok pravdivý, tak skúšku z vypočítateľnosti nik nespraví.“.

Takže, čo vlastne vieme?
– platí A, lebo z toho sme vychádzali
– platí „ak A, tak B“, lebo je to to isté ako A
– a teda podľa modus ponens platí B, zbaľte sa a choďte domov `:-)`

V čom je problém? Curryho paradox nám vlastne hovorí niečo o tom, ako musia vyzerať bezosporné formálne dokazovacie systémy. Na rozdiel od prirodzenej reči musí v každom takomto systéme platiť, že ak `Y` je nedokázateľné tvrdenie, tak nemôže existovať žiadne `X` také, že `X` je ekvivalentné `X→Y`.

1.9 Myšlienka Gödelovho dôkazu

Gödelov dôkaz prvej vety o neúplnosti je založený na jednoduchej myšlienke: Zostrojí tvrdenie, ktoré hovorí „som nedokázateľné“. Presnejšie, ukáže, že ak si očíslujeme všetky syntakticky korektné reťazce predstavujúce tvrdenia, tak nutne bude existovať také n, že reťazec n zodpovedá tvrdeniu „tvrdenie číslo n je nedokázateľné“.

Z predpokladu konzistentnosti dostaneme, že toto tvrdenie skutočne musí byť nedokázateľné. Na dôkaz toho, že je aj nevyvrátiteľné (neexistuje dôkaz reťazca predstavujúceho jeho negáciu), potrebujeme o trochu silnejšiu požiadavku na náš formálny systém: ω-konzistenciu.

Hovoríme, že formálny systém je ω-konzistentný, ak neexistuje reťazec R s voľnou premennou `x` taký, že pre každé n je dokázateľný reťazec R_n (ktorý vznikne tak, že za každý výskyt `x` dosadíme reťazec predstavujúci prirodzené číslo n), ale zároveň je dokázateľný reťazec $\exists$`x(¬(`R`))`.

Detailnejší popis dôkazu viď napr. http://en.wikipedia.org/wiki/G%C3%B6del%27s_second_incompleteness_theorem#Proof_sketch_for_the_first_theorem

Voľne podľa Zlatoša:

Uvažujme konkrétnu teóriu T. Všetky formuly, t.j. výrokové formy, s najviac jednou voľnou premennou si efektívne očíslujeme; taktiež efektívne očíslujeme dôkazy. Budeme písať $\varphi_n(x)$ pre formulu a Δ_z pre dôkaz.

Predpokladajme, že v našej teórii máme trojmiestny predikát $P(m, n, z)$ taký, že keď za m, n a z dosadíme vhodné reťazce, dostaneme výrok „z je číslom dôkazu tvrdenia, ktoré dostaneme, ak do formuly číslo n dosadíme m“.

Potom reťazec `(∃z)P(m,n,z)` je formalizáciou tvrdenia „existuje dôkaz tvrdenia $\varphi_n(m)$“.

Ak je v našej teórii dokázateľné tvrdenie $\varphi_n(m)$, tak je dokázateľné aj `(∃z)P(m,n,z)`. Tvrdenie totiž má dôkaz, ten dôkaz má svoje číslo, tomu číslu prislúcha reťazec `zz`, pre ktorý je dokázateľné `P(m,n,zz)` a odtiaľ aj pôvodná formula.

Obrátená implikácia však platí práve len v ω-konzistentných teóriách. Problém je v tom, že náš dôkaz `(∃z)P(m,n,z)` nemusí byť konštruktívny. A v takom prípade potrebujeme záruku, že keď začneme (my, mimo formálneho systému) prezerať všetky prirodzené čísla a dosádzať reťazce, ktoré ich predstavujú, tak časom nájdeme jeden, pre ktorý to zafunguje.

Intuitívny príklad, kedy ω-konzistentnosť a konzistentnosť nie je to isté: Vieme dokázať tvrdenie „neplatí, že celý prvý kvadrant nekonečnej štvorcovej siete je biely“, lenže zároveň vieme pre každé n dokázať, že políčko $(n, 0)$ biele je. Vo formálnom systéme sa na to treba dívať nasledovne: nič zvonka nám nezaručí, že reťazce `0`, `1`, `(1+1)`, `((1+1)+1)`, atď. skutočne pokrývajú všetky možnosti. Čo, ak má ten formálny systém v našom svete aj iný model ako prirodzené čísla?

1.10 Random trivia

Rosserov trik. Vylepšená verzia Gödelovho tvrdenia ktorá nevyžaduje ω-bezospornosť, iba obyčajnú bezospornosť teórie. Rosserovo pravdivé ale nedokázateľné tvrdenie je formalizáciou výroku „ak existuje môj dôkaz a má číslo d, tak existuje aj dôkaz mojej negácie a má číslo menšie ako d“.

Churchovo pozorovanie. Pre ľubovoľnú teóriu obsahujúcu Peanovu aritmetiku (http://en.wikipedia.org/wiki/Peano_arithmetic) nie je množina dokázateľných tvrdení rekurzívna.

Tarského veta o nedefinovateľnosti pravdy. Pre ľubovoľnú teóriu obsahujúcu Peanovu aritmetiku platí, že v rámci teórie nevieme definovať unárny predikát, ktorý by bol pravdivý práve pre čísla tvrdení, ktoré sú formalizáciou pravdivých tvrdení v aritmetike prirodzených čísel. Viac na http://en.wikipedia.org/wiki/Tarski%27s_undefinability_theorem

Násobenie treba. Pressburgerova aritmetika je Peanova aritmetika bez symbolu pre násobenie. (Máme teda ako axiómy len definíciu sčítania a matematickú indukciu.) Táto aritmetika ešte neumožňuje sformulovať Gödelovo tvrdenie. A naopak, vie sa o nej, že je konzistentná, úplná a navyše je dokázateľnosť tvrdenia v Pressburgerovej aritmetike rozhodnuteľná. (Optimálny algoritmus rozhodujúci dokázateľnosť tvrdenia má časovú zložitosť rádovo $2^{2^{cn}}$, kde $c > 0$ je konštanta a n dĺžka vstupného reťazca.)